IPQS Expands its Cybersecurity Product Suite to Combat Zero-Day Threats and Leaked Identity Credentials

IPQS announces its expanded cybersecurity offerings at RSA Conference 2024.

SAN FRANCISCO, CALIFORNIA, UNITED STATES, May 8, 2024 /EINPresswire.com/ -- IPQS, a trusted global provider for fraud prevention and cybersecurity, has unveiled its expanded cybersecurity product suite at RSA Conference 2024. IPQS has launched a versatile toolkit to address today's most prevalent attack vectors, including zero-day malware, phishing, and leaked identity credentials.

With more business operations moving online, the number of routes available for cyberattacks has risen dramatically. However, budgets and resources are failing to grow at the same pace as attacks. Businesses need a cost-effective way to protect their organizations, and fight zero-day threats that are bypassing other solutions.

IPQS is helping businesses solve these critical security challenges while safeguarding their budgets. Its newly launched tools include a file scanner which detects advanced malware, a URL scanner to detect malicious links, and a dark web service that gives insight into leaked identity credentials.

Protect Against Zero-Day Malware
The IPQS File Malware Scanner is a game-changer in the defense against advanced cyber threats. It identifies elusive zero-day threats by executing any file within a secure environment using temporary virtual machines. This detects hidden threats by observing the file's true behavior. With IPQS, businesses can easily scan any file, document, or image without friction or delays. The malware scanner operates in real time, and can be integrated into application workflows through an API.

Detect Malicious Links
The IPQS Malicious URL Scanner is a crucial tool in detecting dangerous links within user generated content, emails, and webpages. It inspects links in real-time for phishing, viruses, and reputational risks. IPQS will analyze links and provide granular information on the complete risk profile of a URL. IPQS has exceptional insight into the behavioral traits and forensic details of suspicious links. Advanced algorithms can match indicators from other malicious domains to identify emerging threats.

Data Breach Search Engine
The IPQS Leaked Data Verification solution alerts companies to email addresses, usernames, and passwords that have been breached online. This information is leveraged to protect user accounts and keep internal systems secure. IPQS engineers work tirelessly to maintain one of the industry's most exhaustive databases on leaked data. It pools insights from a vast collection of repositories from across the internet and actively scans the dark web for fresh information. Advanced matching techniques will pinpoint leaked data and link it with inquiries with exceptional accuracy.

IPQS Platform: Solving Top Security and Fraud Concerns
These new capabilities are part of a comprehensive set of IPQS solutions that tackle fraud, bots, cyberthreats, account security, and identity abuse. IPQS provides actionable insight into evolving risk signals for more accurate attack detection. It runs the world's largest honeypot network, which analyzes malicious traffic at scale. This offers exceptional visibility into emerging threats to support security and fraud teams.

About IPQS
IPQS is a trusted platform to combat fraud and cyberthreats in all their forms, using accurate and timely intelligence. The platform combines IP and device fingerprinting, and email and phone validation, and cyberthreat detection. More than 3,500 companies, including many Fortune 500 businesses, rely on IPQS for risk mitigation, enhanced deliverability, and reduced abuse.

Lizzie Clitheroe
IPQS
+1 877-968-2710
email us here
Visit us on social media:
Twitter
LinkedIn
